Políticas de Seguridad DLP y Restricción de Dispositivos USB

# Políticas de Seguridad DLP (Prevención de Pérdida de Datos)

## Introducción al Data Loss Prevention (DLP)

La Prevención de Pérdida de Datos (DLP) es un conjunto de políticas y tecnologías diseñadas para detectar, monitorear y proteger la información sensible contra accesos no autorizados, filtraciones y exfiltración accidental o maliciosa. Su implementación es fundamental en una organización para cumplir con regulaciones, evitar pérdidas económicas y proteger la reputación institucional. DLP garantiza que los datos críticos estén disponibles solo para quienes los necesitan según su rol y responsabilidad.

## Clasificación de Datos

La organización establecerá una clasificación de datos en tres niveles:

1. Datos Públicos: Información que puede ser compartida abiertamente, como materiales promocionales, boletines o contenidos en la página web.

2. Datos Internos: Información operativa que no debe divulgarse fuera de la organización, como manuales internos o políticas de RRHH.

3. Datos Sensibles: Datos que requieren la máxima protección, como información financiera, datos personales identificables (PII) y propiedad intelectual.

## Acceso y Control (Principio del Menor Privilegio)

El acceso a los datos se gestionará aplicando el principio del menor privilegio, garantizando que cada usuario solo tenga acceso a la información estrictamente necesaria para desempeñar sus funciones.  
  
Flujo de revisión:  
- Los responsables de equipo solicitarán permisos.  
- El equipo de TI y seguridad validará las solicitudes.  
- Las revisiones de permisos se realizarán trimestralmente.  
- Se llevará un registro en una plataforma de control de accesos (AWS IAM como ejemplo Cloud).

## Monitoreo y Auditoría

Todas las interacciones con datos sensibles serán monitoreadas y auditadas mediante herramientas especializadas:  
  
Herramientas:  
- SIEM (como Splunk o Azure Sentinel) para detectar patrones sospechosos.  
- Soluciones DLP (como Microsoft Purview o Symantec DLP) para rastrear datos en movimiento, en uso y en reposo.  
  
Se generarán informes periódicos y alertas en tiempo real ante eventos críticos (copias no autorizadas, accesos fuera del horario laboral, etc.).

## Prevención de Filtraciones

Para proteger los datos sensibles, se implementarán las siguientes medidas:  
- Cifrado: Todos los datos sensibles estarán cifrados en tránsito y en reposo (TLS, AES-256).  
- Herramientas DLP: Detectarán intentos de copiar o mover datos sensibles fuera de entornos permitidos.  
- Bloqueo de canales no autorizados, como almacenamiento en la nube no aprobado o correo personal.

## Educación y Concientización

La capacitación del personal es clave para una política DLP efectiva. Se implementará un programa de concientización que incluye:  
- Cursos trimestrales sobre ciberseguridad y uso responsable de datos.  
- Simulaciones de fuga de datos y ataques de phishing.  
- Política de firma de compromiso con el cumplimiento de las políticas de seguridad.

# Implementación de Políticas de Restricción de Dispositivos USB

## Configuración en Máquina Virtual (VirtualBox)

1. Instalación del Extension Pack para soporte USB.  
2. Activación del controlador USB 2.0 o 3.0 en configuración de la VM.  
3. Conexión del dispositivo USB físico a la VM desde el menú Dispositivos > USB.

## Restricción de Dispositivos USB en Windows

1. Abrir gpedit.msc.  
2. Navegar a: Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento removible.  
3. Activar las siguientes políticas:  
 - Denegar acceso de lectura a discos extraíbles  
 - Denegar acceso de escritura a discos extraíbles  
4. Reiniciar la VM para aplicar los cambios.

## Validación de la Política USB

1. Crear un usuario regular sin privilegios administrativos.  
2. Iniciar sesión con ese usuario.  
3. Conectar el USB → Se mostrará un mensaje de denegación de acceso si la política fue aplicada correctamente.

## Excepciones para Usuarios Específicos (Investigación)

Para habilitar excepciones:  
  
1. Iniciar sesión con un usuario administrador.  
2. En el Editor de Políticas de Grupo, usar la directiva: Filtrado de seguridad en las propiedades de la política para aplicar solo a grupos específicos.  
3. Alternativamente, usar gpedit.msc combinado con permisos en gpupdate /force y GPO a nivel de Active Directory.  
  
Verificación: Iniciar sesión con un usuario autorizado y confirmar que tiene acceso al USB, mientras que los usuarios estándar no.